Cloudsquid Data Processing Agreement

DATA PROCESSING AGREEMENT ACCORDING TO ART. 28 GDPR

SECTION I

Clause 1

Purpose and scope

a) These Standard Contractual Clauses (hereinafter "Clauses") are intended to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, for free movement of data and repealing Directive 95/46/EC.

b) The Controllers and Processors listed in Annex I have agreed to these clauses to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725 .

c) These clauses apply to the processing of personal data in accordance with Annex II.

d) Schedules I to IV form part of the Clauses.

and) These clauses are without prejudice to the obligations to which the Controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These clauses do not, by themselves, ensure compliance with the obligations relating to international data transfers set out in Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Unchangeability of the clauses

a) The parties undertake not to modify the clauses, except to supplement or update the information provided in the appendices.

b) This does not prevent the parties from incorporating the standard contractual clauses set out in these clauses into a more extensive contract and from adding further clauses or additional guarantees, provided that they do not directly or indirectly contradict the clauses or restrict the fundamental rights or freedoms of the data subjects.

Clause 3

Interpretation

a) Where these clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, these terms have the same meaning as in the relevant Regulation.

b) These clauses must be interpreted in the light of the provisions of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 respectively.

c) These clauses may not be interpreted in a way that is contrary to the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or which restricts the fundamental rights or freedoms of the data subjects.

Clause 4

Priority

In the event of any conflict between these clauses and the terms of any related agreement existing or subsequently entered into or concluded between the parties, these clauses shall prevail.

Clause 5 – Optional

Coupling clause

a) An entity that is not a party to these clauses may, with the consent of all parties, accede to these clauses at any time as a Controller or as a Processor by completing the annexes and signing Annex I.

b) After completing and signing the annexes referred to in point (a), the acceding entity will be treated as a party to these clauses and will have the rights and obligations of a Controller or a Processor as referred to in Annex I.

c) No rights or obligations arising from these clauses apply to the acceding institution for the period prior to its accession as a party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the Controller, are set out in Annex II.

Clause 7

Obligations of the parties

7.1 Instructions

a) The Processor will only process personal data on documented instructions from the Controller, unless he is obliged to process it under Union law or the law of a Member State to which he is subject. In such a case, the Processor will inform the Controller of these legal requirements before processing, unless the law in question prohibits this because of an important public interest. The Controller may issue further instructions throughout the processing of personal data. These instructions must always be documented.

b) The Processor shall inform the Controller immediately if it considers that instructions given by the Controller violate Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable Union or Member State data protection rules.

7.2 Purpose limitation

a) The Processor will only process the Personal Data for the specific purpose(s) set out in Annex II, unless it receives further instructions from the Controller.

b) The Processor is expressly prohibited from using any Personal Data processed on behalf of the Controller, including any data uploaded by the Controller or its users to the Services, to train or improve any artificial intelligence models, machine learning models, or any similar systems for the Processor or any third party. This prohibition shall survive the termination of the agreement.

7.3 Duration of processing personal data

The data will only be processed by the Processor for the duration specified in Appendix II.

7.4 Security of processing

a) The Processor shall take at least the technical and organizational measures listed in Annex III to ensure the security of the personal data. This includes protecting the data from a breach of security that, whether accidental or unlawful, results in the destruction, loss, alteration or unauthorized disclosure of or access to the data (hereinafter “personal data breach”)). When assessing the appropriate level of protection, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, circumstances and purposes of the processing and the risks associated with data subjects.

b) The Processor shall grant its staff access to the personal data subject to processing only to the extent strictly necessary for the implementation, management and monitoring of the contract. The Processor guarantees that the persons authorized to process the personal data received have committed themselves to confidentiality or are subject to an appropriate legal obligation of confidentiality.

7.5 Sensitive Data

If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, or genetic data or biometric data for the purpose of uniquely identifying a natural person, data relating to health, sexual life or contain the sexual orientation of a person or data about criminal convictions and offenses (hereinafter “sensitive data”), the Processor will apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance with the clauses

a) The parties must be able to demonstrate compliance with these clauses.

b) The Processor will promptly and appropriately process requests from the Controller regarding the processing of data in accordance with these clauses.

c) The Processor shall provide the Controller with all the information necessary to demonstrate compliance with the obligations set out in these clauses and arising directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the request of the Controller, the Processor shall also permit and contribute to the audit of the processing activities covered by these clauses at appropriate intervals or when there are signs of non-compliance. When deciding on a review or audit, the Controller may take relevant certifications of the Processor into account.

d) The person responsible can carry out the audit himself or commission an independent auditor. The audits may also include inspections of the Processor's premises or physical facilities and may be carried out with reasonable notice.

and) The parties shall make the information referred to in this clause, including the results of audits, available to the relevant supervisory authority(s) upon request.

7.7 Use of sub-Processors

a) The Processor has the general authorization of the Controller to engage sub-Processors included in an agreed list. The Processor will expressly inform the Controller in writing at least two weeks in advance of any intended changes to this list by adding or replacing sub-Processors, thereby allowing the Controller sufficient time to object to these changes before engaging the relevant sub-Processor(s). The Processor provides the Controller with the necessary information so that the Controller may exercise the right to object.

b) Right to Object. The Controller may reasonably object to the new sub-Processor in writing within ten (10) business days of the notice. Any objection must explain how the use of the proposed sub-Processor would violate Applicable Data-Protection Law or materially reduce the security of the Services.

c) Good-faith Resolution. If the Controller submits a timely and reasoned objection, the Parties will confer in good faith to find a mutually acceptable solution. The Processor may

recommend a commercially reasonable change to the Services or the Controller's configuration to avoid processing by the objected-to sub-Processor, or elect not to use the new sub-Processor for the Controller's Personal Data.

d) Limited Termination Right. If no mutually acceptable solution is reached within thirty (30) days of the Processor’s receipt of the objection, the Controller may terminate, without penalty, only those Service components that cannot be provided without the objected-to Sub-Processor by giving written notice. The Processor will refund any unused prepaid fees for the terminated components. This is the Controller’s sole and exclusive remedy for any objection to a new Sub-Processor.

e) If the Processor engages a sub-Processor to carry out certain processing activities (on behalf of the Controller), this engagement must be carried out by means of a contract which imposes on the sub-Processor substantially the same data protection obligations as those applicable to the Processor under these clauses. The Processor shall ensure that the Sub-Processor complies with the obligations to which the Processor is subject in accordance with these clauses and in accordance with Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) The Processor will provide the Controller with a copy of such subcontracting agreement and any subsequent changes upon its request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the Agreement before disclosing a copy.

d) The Processor is fully liable to the Controller for ensuring that the sub-Processor fulfils its obligations in accordance with the contract concluded with the Processor. The Processor notifies the Controller if the sub-Processor does not fulfil its contractual obligations.

and) The Processor agrees with the sub-Processor to a third-party beneficiary clause, according to which the Controller - in the event that the Processor ceases to exist in fact or in law or becomes insolvent - has the right to terminate the sub-contract and order the sub-Processor to delete or return the personal data.

7.8 International data transfers

a) Any transfer of data by the Processor to a third country or an international organization shall be carried out solely on the basis of documented instructions from the Controller or to comply with a specific provision under Union law or the law of a Member State to which the Processor is subject, and shall comply with Chapter V of the Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The Processor shall ensure that any such transfer is made, in the first instance, to a country that is the subject of an adequacy decision by the European Commission under

Article 45 of Regulation (EU) 2016/679.

c) Where no adequacy decision exists for the destination country, the Processor and any relevant sub-Processor shall ensure compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided that the requirements for the application of these standard contractual clauses are met.

Clause 8

Support for those responsible

a) The Processor shall immediately inform the Controller of any request received from the data subject. He does not answer the request himself unless he has been authorized to do so by the person responsible.

b) Taking into account the type of processing, the Processor supports the Controller in fulfilling his obligation to respond to data subjects' requests to exercise their rights. When fulfilling its obligations under letters a and b, the Processor follows the instructions of the Controller.

c) In addition to the Processor's obligation to assist the Controller in accordance with clause 8(b), the Processor, taking into account the nature of the data processing and the information available to it, shall also assist the Controller in complying with the following obligations:

1) Obligation to carry out an assessment of the impact of the proposed processing operations on the protection of personal data (hereinafter “data protection impact assessment”) where a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2) Obligation to consult the relevant supervisory authority(s) before processing if a data protection impact assessment shows that the processing would result in a high risk unless the Controller takes measures to mitigate the risk;

3) Obligation to ensure that the personal data is accurate and up-to-date by informing the Controller without delay if the Processor discovers that the personal data it is processing is inaccurate or out of date;

4) Obligations under Article 32 of Regulation (EU) 2016/679.

1. d) The parties shall specify in Annex III the appropriate technical and organizational measures to support the Controller by the Processor in the application of this clause, as well as the scope and extent of the support required.

Clause 9

Notification of personal data breaches

In the event of a personal data breach, the Processor shall cooperate with and provide appropriate assistance to the Controller to ensure that the Controller fulfills its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of the processing and the information available to the Processor.

9.1 Breach of protection of data processed by the Controller

In the event of a personal data breach related to the data processed by the Controller, the Processor shall assist the Controller as follows:

a) upon promptly reporting the personal data breach to the relevant supervisory authority(s) after the breach has become known to the Controller, where relevant (unless the personal data breach is unlikely to result in a risk to the personal rights and freedoms of natural persons);

b) when obtaining the following information to be included in the Controller's report in accordance with Article 33(3) of Regulation (EU) 2016/679, which information must include at least the following:

1) the type of personal data, where possible, indicating the categories and approximate number of data subjects concerned and the categories and approximate number of personal data sets concerned;

2) the likely consequences of the personal data breach;

3) the measures taken or proposed by the Controller to remedy the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

If and to the extent that all such information cannot be provided at the same time, the initial report will contain the information available at that time and additional information, as it becomes available, will thereafter be provided without unreasonable delay;

c) when complying with the obligation referred to in Article 34 of Regulation (EU) 2016/679, to notify the data subject without undue delay of the personal data breach where that breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Breach of protection of data processed by the Processor

In the event of a personal data breach related to the data processed by the Processor, the Processor shall report this to the Controller without undue delay and in any event no later than 48 hours after becoming aware of the breach. This message must contain at least the following information:

a) a description of the nature of the breach (preferably indicating the categories and the approximate number of individuals affected and the approximate number of records

affected);

b) Contact details of a contact point where further information about the personal data breach can be obtained;

c) the likely consequences and the measures taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.

If and to the extent that all such information cannot be provided at the same time, the initial report will contain the information available at that time and additional information, as it becomes available, will be provided thereafter without undue delay.

The parties shall set out in Annex III any other information to be provided by the Processor to assist the Controller in carrying out its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Violations of the clauses and termination of the contract

a) If the Processor fails to comply with its obligations under these clauses, the Controller may - without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 - instruct the Processor to suspend the processing of personal data until it complies with these clauses or the contract is terminated. The Processor will inform the Controller immediately if, for whatever reason, it is unable to comply with these clauses.

b) The Controller is entitled to terminate the contract insofar as it concerns the processing of personal data in accordance with these clauses if

1) the Controller has suspended the processing of personal data by the Processor in accordance with point (a) and compliance with those clauses has not been restored within a reasonable period of time, but in any event within one month of the suspension;

2) the Processor materially or persistently breaches these clauses or fails to comply with its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

3) the Processor fails to comply with a binding decision of a competent court or supervisory authority(s) relating to its obligations under these Clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The Processor is entitled to terminate the Contract insofar as it concerns the processing of Personal Data in accordance with these clauses if the Controller insists on carrying out its instructions after being informed by the Processor that its instructions violate applicable legal requirements in accordance with clause 7.1 letter b violated.

d) Upon termination of the contract, the Processor shall, at the Controller's option, delete all personal data processed on behalf of the Controller and certify to the Controller that this has been done, or return all personal data to the Controller and delete existing copies, unless required by Union law or There is an obligation to store personal data under Member State law. The Processor continues to ensure compliance with these clauses until the data is deleted or returned.

Confirmation & Acceptance

Cloudsquid GmbH			_____	
Signature	_____		Signature	_____
Name	_____		Name	_____
Date	_____		Date	_____

APPENDIX I – LIST OF PARTIES

Responsible person: [Name and contact details of the person responsible and, if applicable, the data protection officer of the person responsible]

1. Name:

Address:

Name, function and contact details of the contact person:

Processor: [Name and contact details of the Processor(s) and, if applicable, the data protection officer of the Processor]

1. Name: Cloudsquid GmbH

Address: Cloudsquid GmbH, Schönhauser Allee 180, 10119 Berlin

Name, function and contact details of the contact person:

Filip Rejmus, CPO

filip@cloudsquid.io

APPENDIX II – DESCRIPTION OF PROCESSING

Categories of data subjects whose personal data are processed

- Employees of the Controller.

- Further categories of Data Subjects, depending on the Controller's use of the Services.

Categories of personal data processed:

- User Account related data such as name, username/ID, contact details, log and protocol data.
- Further categories of Personal Data, depending on the Controller's use of the Services

Type of processing

- Provision of the Cloudsquid Service: The Cloud Service provides tools and features to integrate and automate various third-party applications, websites and services maintained by the Controller. Personal Data is primarily used to provide access to the Service by the Processor. If Personal Data is used for application-related usage analysis, the data will be anonymized.
- Data extraction Service: The Data extraction service extracts and stores data on Processor Infrastructure. Personal Data is potentially present in Documents originating from the Controller and depends on the Controller’s use of the service.

Purpose(s) for which the personal data is processed on behalf of the Controller

- Rendering of the Services by the Processor to the Controller, as agreed in the Agreement between the parties.
- Processing initiated by Users in the course of their use of or access to the Services.
- Processing to comply with other reasonable and documented instructions provided by the Controller that are consistent with the terms of the Agreement.

Duration of processing:

- The duration of the Processing equals the applicable Subscription Term.

Legal retention periods:

If necessary, data will be retained for the periods required by law.